Gaining the Initiative in Cyberspace: Why the DoD Needs a Cyber Military Branch

Paul E. Baker, Captain, US Army

CG-16, Expeditionary Warfare School, Marine Corps University

February 16, 2016

Over the last 15 years, cyber-attacks on civilian and military organizations have increased exponentially, causing cybersecurity to become a growing concern for United States businesses and the Department of Defense. In 2015 alone, there were an average of 160 successful cyber-attacks per week on US companies,[1] and in September of that year, the US military discovered that Chinese hackers stole terabytes of sensitive data from US defense contractors.[2] In 2009, in an attempt to prevent such attacks, then-Defense Secretary Robert M. Gates established the US Cyber Command as a functional sub-unified command[3] with the mission to ensure Department of Defense (DoD) mission assurance, deter or defeat strategic threats to US interests and infrastructure, and achieve the Joint Force Commander's objectives.[4] Since its development, US Cyber Command has worked diligently to fill its 133 cyber mission teams with qualified cyber operators. These teams would be broken out into 68 cyber protection teams, 13 national mission teams, 27 combat mission teams, and 25 support teams. Originally, the DoD modelled US Cyber Command after US Special Operations Command, in that each service retained their own cyber capabilities,[5] with a single joint commander (dual-hatted as the director of the National Security Agency) to coordinate and focus the cyber warfare mission. With this current model, US Cyber Command is not organized to effectively conduct either offensive or defensive operations in cyberspace, and thus many independent researchers believe that the United States is losing the cyber war.[6] To gain the initiative in the cyber domain, the United States should create a new cyber military branch: the US Cyber Corps. The US Cyber Corps, specifically focused on cyberspace operations, will improve the command relationship with the DoD and President of the United States, create a common initial training pipeline for cyber operators, and enable cyber operators to better maintain their operational capabilities in order to establish the United States as the dominant cyber force in the world.

In US Cyber Command's current layout, the Cyber Command Commander is not a part of the Joint Staff and does not directly advise the Secretary of Defense or the President on matters involving operations in cyberspace.[7] Therefore, the Joint Staff has no true ability to strategically plan for cyberwarfare. The creation of a US Cyber Corps will subsequently create a military service chief – a Chief of Staff of the Cyber Corps. Military service chiefs, as members of the Joint Chiefs of Staff, "offer advice to the President, the Secretary of Defense, and the National Security Council."[8] Also of benefit, this military service chief would be a four-star equivalent and have equal representation amongst the other major military services. Currently, the Joint Staff can coordinate with US Strategic Command, and then down to US Cyber Command,[9] but this is an unnecessary sequence of communication that leaves room for error and inefficiency. Establishing a US Cyber Corps, including an appropriate military service chief, would drastically improve the ability of the President, Secretary of Defense, and Chairman of the Joint Chiefs of Staff to understand the operations in cyberspace and plan for future operations by centralizing intelligence and strategy.

Coupled with the inefficiency of US Cyber Command's chain of command, US Cyber Command is also at a disadvantage when it comes to training its cyber operators. Each major DoD headquarters manages or commands the programs and operations of the DoD, the DoD components, and their major military units.[10] The major DoD headquarters have numerous responsibilities, including training and education.[11] Currently, the US Army, Navy, and Air Force's cyber operators each attend training at different schools, with different courses and various learning outcomes. The US Army trains all cyber officers, warrant officers, and enlisted soldiers at the US Army Cyber School in Fort Gordon, Georgia. The US Navy trains enlisted sailors as Network Cryptologic Technician[12] at the six-month long Joint Cyber Analysis Course

at Corry Station, Pensacola, Florida.[13] The US Air Force trains officers at a 23-week undergraduate cyberspace training course[14] and enlisted Airmen at a 17-week cyber defense operations course, both at Keesler Air Force Base, Mississippi.[15] As a result of the varying course lengths and training plans, cyber operators leave their training with a different understanding of cyberwarfare than their joint partners. Following each service's individualized training, the cyber operators are brought together to begin training as one of the 133 cyber mission teams. This approach does not enable US Cyber Command to bring their cyber operators into the same mission quickly because of the excess time needed to train up these teams. By establishing the US Cyber Corps, all cyber operators would follow the same training and education pipeline before being assigned to one of the cyber mission teams. Even if the incoming cyber operators had different backgrounds, they would have a shared vernacular and speak the same language, enabling the cyber mission teams to operate in the cyber domain quicker.

In addition to the cyber-specific training requirements that each cyber operator needs to master, each individual service mandates that their service members maintain service-specific skills as well. These skills are not necessary for cyber operators because they do not directly translate to skills employed in cyberwarfare. For the US Army, some of these requirements include semiannual physical readiness training (including combatives) and weapons qualification.[16] The US Army also prescribes individual and team battle drills "known to be critical to Soldier survival."[17] These tasks include conducting first aid, operating in an urban environment, and evacuating injured personnel from a vehicle. The Army does not require commanders to train their soldiers on every individual and team battle drill, however it is expected that all Soldiers know how to perform these tasks. Unlike the current major services,

cyber operators do not need to be in top physical fitness or know how to perform first aid to meet the demands of their job. Cyber operators need to understand how computers and networks work, and how to use their assigned tools in this environment. As an alternative, the semiannual requirements of a cyber operator may include the speed to hack a network or a test of different computer operating languages. The creation of a US Cyber Corps removes the unnecessary required training of each military service and allows the cyber mission teams to focus on maintaining their cyber-specific training.

Critics view cyber warfare as a component of combined arms and therefore assert that tactical commanders need to have the ability to affect the enemy's cyber infrastructure. General Keith Alexander, the first Commander of US Cyber Command, believed "that the [cyber] forces needed to be embedded in tactical configurations, and if they needed to do that, the services should be involved."[18] General Alexander's belief that cyber forces would work attached to tactical units supported the development of US Cyber Command off the US Special Operations Command model. However, this logic hinged on the belief that cyber operators would be effective within tactical units. In fact, cyber operators do not need to be embedded in tactical forces because their mission does not take place in the physical environment. Cyber mission teams need the ability to access computers, switches, routers, servers, and firewalls to defend and maintain friendly networks, and to attack enemy networks. These switches, routers, servers, and firewalls can be accessed remotely from a distant location. As each service does not have the authority or infrastructure to conduct cyber-attacks from forward tactical elements, it is extremely inefficient to attach stationary cyber mission teams to mobile maneuver forces.

In today's interconnected environment, there are approximately 3.17 billion internet users around the world,[19] and research estimates that there will be 38.5 billion "things" – computers,

phones, homes, fridges, cars, etc. – connected to the internet by 2020.[20] The cyber domain is extremely large and complex and the United States needs a cyber-specific military service to address these issues. The United States is spending a lot of time and resources to mitigate the damage that foreign entities are creating in the cyber domain. This has led many to say that the US is losing the cyberwar.[21] Now is the time to create a new military service to be able to respond to the challenges in cyberspace. The creation of a new cyber branch will bring some growing pains. The equipment, facilities, doctrine, and personnel could all be transferred from US Cyber Command into the US Cyber Corps. A harder problem to sort out is the legal authorities that go with the establishment of a new branch, whose domain runs between public, private, and military networks. However, the benefits to this cyber branch outweigh the concerns. The US Cyber Corps would improve the DoD's ability to control operations in cyberspace, streamline training pipelines for cyber operators, and allow the cyber operators to focus on tasks directly related to cyberspace. In the 1940s, the US separated the US Air Force from the US Army due to changes in technology and to improve command relationships. This separation helped to bring about the air supremacy that the United States has enjoyed for the last 60 years. It is time to create a US Cyber Corps to meet today's technological changes and to bring about an era of US cyberspace supremacy.

Notes

1. Riley Walters, "Cyber Attacks on U.S. Companies Since November 2014," *The Heritage Foundation*, no. 4487 (2015), http://report.heritage.org/ib4487.

2. Lisa Brownlee, "Report: Chinese Hackers Used OPM Data To Steal US Military Intel; 'Significant Risk To US Military'," *Forbes,* September 19, 2015, http://www.forbes.com/sites/lisabrownlee/2015/09/19/report-chinese-hackers-used-opm-data-to-steal-us-military-intel-significant-risk-to-us-military/#5e98ced71800/.

3. Joe Gould, "Former NSA Chief: Follow SOCOM Model for Cyber," *Defense News*, April 17, 2015, http://www.defensenews.com/story/defense-news/blog/intercepts/2015/04/17/keith-alexander-cyber-dod-aei/25951903/.

4. Michael S. Rogers, "Beyond the Build: Delivering Outcomes through Cyberspace. The Commander's Vision and Guidance for US Cyber Command," United States Cyber Command, June 3, 2015.

5. William Jackson, "DOD creates Cyber Command as U.S. Strategic Command subunit: New post will defend .mil domain," *Federal Computer Week,* June 24, 2009, https://fcw.com/Articles/2009/06/24/DOD-launches-cyber-command.aspx.

6. Gary S. Miliefsky, "Red Alert: America is Losing The CyberWar!" *Cyber Defense Magazine*, August 7, 2015, http://www.cyberdefensemagazine.com/red-alert-america-is-losing-the-cyberwar/.

7. Directorate for Organizational and Management Planning/ Office of the Director of Administration and Management/ Office of the Secretary of Defense, *Organization of the Department of Defense,* March 2012.

8. About the Joint Chiefs of Staff, Joint Chiefs of Staff, accessed February 10, 2016, http://www.jcs.mil/About.aspx.

9. *Organization of the Department of Defense*.

10. US Department of Defense, *Major DoD Headquarters Activities,* Instruction 5100.73, December 1, 2007, 12-15.

11. Ibid., 15.

12. Cryptologic Technician – Networks (CTN), Navy Personnel Command, last modified April 10, 2015, http://www.public.navy.mil/bupers-npc/enlisted/community/crypto_it/Pages/CTN.aspx.

13. Thom Seith, "Joint Cyber Analysis Course Challenges New and Veteran Sailors," Center for Information Dominance Public Affairs, January 22, 2015, http://www.navy.mil/submit/display.asp?story_id=85292.

14. Headquarters US Air Force, *Career Field Education and Training Plan: AFSC 17X Cyberspace Operations Officer,* CFETP 17X Parts I and II, (Washington, DC: Department of the Air Force, June 1, 2015).

15. Oriana Pawlyk, "Cyber: The safest job in the Air Force?" *Military Times,* February 20, 2014, http://www.militarytimes.com/story/military/archives/2014/02/20/cyber-the-safest-job-in-the-air-force-/78543786/.

16. Headquarters, Department of the Army, *Army Training and Leader Development,* AR 350-1 (Washington, DC: Department of the Army, August 19, 2014), 167.

17. Headquarters, Department of the Army, *Soldier's Manual of Common Tasks: Warrior Skills Level 1,* STP 21-1-SMCT (Washington, DC: Department of the Army, August 2015).

18. Gould, "Former NSA Chief: Follow SOCOM Model for Cyber."

19. "Number of worldwide internet users from 2000 to 2015 (in millions)," Statista – The Statistics Portal, accessed February 10, 2016, http://www.statista.com/statistics/273018/number-of-internet-users-worldwide/.

20. Sam Smith, "'Internet of Things' Connected Devices to Almost Triple to Over 38 Billion Units by 2020," Juniper Research, July 28, 2015, http://www.juniperresearch.com/press/press-releases/iot-connected-devices-to-triple-to-38-bn-by-2020/.

21. Miliefsky, "Red Alert: America is Losing The CyberWar!"

Bibliography

Boothby, William H. "Methods and Means of Cyber Warfare." *International Law Studies*, vol. 89 (2013). https://www.hsdl.org/?view&did=734393.

Brownlee, Lisa. "Report: Chinese Hackers Used OPM Data To Steal US Military Intel; 'Significant Risk To US Military'." *Forbes*, September 19, 2015. http://www.forbes.com/sites/lisabrownlee/2015/09/19/report-chinese-hackers-used-opm-data-to-steal-us-military-intel-significant-risk-to-us-military/#5e98ced71800/.

Career Browser. U.S. Air Force. Accessed February 9, 2016. http://www.airforce.com/careers/view-all/.

Cryptologic Technician – Networks (CTN). Navy Personnel Command. Last modified April 10, 2015. http://www.public.navy.mil/bupers-npc/enlisted/community/crypto_it/Pages/CTN.aspx.

Denny, Eric J. "The Cyberspace Domain: Path to a New Service?" School of Advanced Military Studies. May 2013.

Directorate for Organizational and Management Planning/ Office of the Director of Administration and Management/ Office of the Secretary of Defense. *Organization of the Department of Defense.* March 2012.

Gould, Joe. "Former NSA Chief: Follow SOCOM Model for Cyber." *Defense News*, April 17, 2015. http://www.defensenews.com/story/defense-news/blog/intercepts/2015/04/17/keith-alexander-cyber-dod-aei/25951903/.

Headquarters, Department of the Army. *Army Training and Leader Development.* AR 350-1. Washington, DC: Department of the Army, August 19, 2014.

Headquarters, Department of the Army. *Soldier's Manual of Common Tasks: Warrior Skills Level 1.* STP 21-1-SMCT. Washington, DC: Department of the Army, August 2015.

Headquarters US Air Force. *Career Field Education and Training Plan: AFSC 17X Cyberspace Operations Officer.* CFETP 17X Parts I and II. Washington, DC: Department of the Air Force, June 1, 2015.

Leed, Maren. "Offensive Cyber Capabilities at the Operational Level: The Way Ahead." *Center for Strategic & International Studies* (2013).

Miliefsky, Gary S. "Red Alert: America is Losing The CyberWar." *Cyber Defense Magazine*, August 7, 2015. http://www.cyberdefensemagazine.com/red-alert-america-is-losing-the-cyberwar/.

Pawlyk, Oriana. "Cyber: The safest job in the Air Force?" *Military Times*, February 20, 2014. http://www.militarytimes.com/story/military/archives/2014/02/20/cyber-the-safest-job-in-the-air-force-/78543786/.

Rogers, Michael S. "Beyond the Build: Delivering Outcomes through Cyberspace. The Commander's Vision and Guidance for US Cyber Command." United States Cyber Command. June 3, 2015.

Seith, Thom. "Joint Cyber Analysis Course Challenges New and Veteran Sailors." Center for Information Dominance Public Affairs. January 22, 2015. http://www.navy.mil/submit/display.asp?story_id=85292.

Smith, Sam. "'Internet of Things' Connected Devices to Almost Triple to Over 38 Billion Units by 2020." Juniper Research, July 28, 2015. http://www.juniperresearch.com/press/press-releases/iot-connected-devices-to-triple-to-38-bn-by-2020/.

Statista. "Number of worldwide internet users from 2000 to 2015 (in millions)." Statista – The Statistics Portal. Accessed February 10, 2015. http://www.statista.com/statistics/273018/number-of-internet-users-worldwide/.

The Armed Forces Communications and Electronics Association. "The Evolution of U.S. Cyber Power." http://www.afcea.org/committees/cyber/documents/TheEvolutionofUSCyberpower.pdf.

US Department of Defense. *Major DoD Headquarters Activities.* Instruction 5100.73, December 1, 2007.

US Department of Defense. "The DoD Cyber Strategy." Washington, DC: April 2015.

US Joint Staff. *Cyberspace Operations.* Joint Publication 3-12 (R). Washington, DC: US Joint Staff, February 5, 2013.

Wall, Andru E. "Demystifying the Title 10-Title 50 Debate: Distinguishing Military Operations, Intelligence Activities & Covert Action." *Harvard National Security Journal,* vol. 3 (2011).

Walters, Riley. "Cyber Attacks on U.S. Companies Since November 2014." *The Heritage Foundation*, no. 4487 (2015). http://report.heritage.org/ib4487.